

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PTO/SB/05 (4/98)

Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Attorney Docket No.

First Inventor or Application Identifier	KIMBEALY J. WELBORN
--	---------------------

Title	COMPUTER VIRUS AVOIDANCE SYSTEM AND MECHANISM
-------	---

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Express Mail Label No. **EK1-79754382 US**

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO:

Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ * Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)
2. ☒ Specification [Total Pages 11]
(preferred arrangement set forth below)
- Descriptive title of the Invention
 - Cross References to Related Applications
 - Statement Regarding Fed sponsored R & D
 - Reference to Microfiche Appendix
 - Background of the Invention
 - Brief Summary of the Invention
 - Brief Description of the Drawings (if filed)
 - Detailed Description
 - Claim(s)
 - Abstract of the Disclosure
3. ☒ Drawing(s) (35 U.S.C. 113) [Total Sheets 2]
4. Oath or Declaration [Total Pages 3]
- a. ☒ Newly executed (original or copy)
 - b. ☐ Copy from a prior application (37 C.F.R. § 1.6
(for continuation/divisional with Box 16 completed)
 - i. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting
inventor(s) named in the prior application
see 37 C.F.R. §§ 1.63(d)(2) and 1.33(f)

5. ☐ Microfiche Computer Program (*Appendix*)
6. Nucleotide and/or Amino Acid Sequence Submission
(*if applicable, all necessary*)
- a. ☐ Computer Readable Copy
- b. ☐ Paper Copy (identical to computer copy)
- c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. ☐ Assignment Papers (cover sheet & document(s))
8. ☐ 37 C.F.R. §3.73(b) Statement ☐ Power of Attorney
(when there is an assignee)
9. ☐ English Translation Document (if applicable)
10. ☐ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
11. ☐ Preliminary Amendment
12. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
- * Small Entity
13. ☒ Statement(s) ☐ Statement filed in prior application,
(PTO/SB/09-12) Status still proper and desired
14. ☐ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
15. ☐ Other: _____

* NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

16. If a **CONTINUING APPLICATION**, check appropriate box, and supply the requisite information below and in a preliminary amendment:
- | | | | |
|---------------------------------------|-------------------------------------|---|--|
| <input type="checkbox"/> Continuation | <input type="checkbox"/> Divisional | <input type="checkbox"/> Continuation-in-part (CIP) | of prior application No. _____ / _____ |
|---------------------------------------|-------------------------------------|---|--|

Prior application information: Examiner

Group / Art Unit:

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

☐ *Customer Number or Bar Code Label*

or ☒ Correspondence address below

(Insert Customer No. or Attach bar code label here)

Name _____

KIMBERLY JOYCE WELBORN

Address

331 SANDPIPER DRIVE

City

DAVIS

State

CA

Zip Code

95616

Country

U.S.A.

Telephone

530.753.7240

 E_2

530,757.9200

Name (Pnnt/Type)

KIMBERLY JOYCE WELBORN

Registration No. (Attorney/Agent)

Signature

Kempster Ave 11th

Da

12/22/1999

Burden Hour Statement This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS** SEND TO Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231

**STATEMENT CLAIMING SMALL ENTITY STATUS
(37 CFR 1.9(f) & 1.27(b))--INDEPENDENT INVENTOR**

Docket Number (Optional)

Applicant, Patentee, or Identifier: KIMBERLY JOYCE WELBORN

Application or Patent No.: _____

Filed or Issued: _____

Title: COMPUTER VIRUS AVOIDANCE SYSTEM AND MECHANISM

As a below named inventor, I hereby state that I qualify as an independent inventor as defined in 37 CFR 1.9(c) for purposes of paying reduced fees to the Patent and Trademark Office described in:

- ☒ the specification filed herewith with title as listed above.
☐ the application identified above.
☐ the patent identified above.

I have not assigned, granted, conveyed, or licensed, and am under no obligation under contract or law to assign, grant, convey, or license, any rights in the invention to any person who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person had made the invention, or to any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern, or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

- ☒ No such person, concern, or organization exists.
☐ Each such person, concern, or organization is listed below.

Separate statements are required from each named person, concern, or organization having rights to the invention stating their status as small entities. (37 CFR 1.27)

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28(b))

KIMBERLY J. WELBORN
NAME OF INVENTOR

CHRISTOPHER M. WELBORN
NAME OF INVENTOR

NAME OF INVENTOR

Kimberly Joyce Welborn
Signature of inventor

Christopher M. Welborn
Signature of inventor

Signature of inventor

12/22/1999
Date

12/22/1999
Date

Date

Patent Application of
Kimberly Joyce Welborn and Christopher Michael Welborn,
U.S. Citizens and Residents of Davis, California, U.S.A.
for a
COMPUTER VIRUS AVOIDANCE SYSTEM AND MECHANISM

TITLE OF INVENTION

Computer Virus Avoidance System and Mechanism

CROSS-REFERENCE TO RELATED APPLICATIONS

Not Applicable

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR
DEVELOPMENT

Not Applicable

REFERENCE TO A MICROFICHE APPENDIX

Not Applicable

BACKGROUND OF THE INVENTION

This invention relates to a computer system that aids in the behavior modification of computer users who unknowingly and innocently spread computer viruses, specifically by

teaching computer users to avoid computer viruses with the use of mock computer viruses and feedback measurements.

The Battle Against Computer Viruses:

Computer viruses pose significant threats to computer systems. Viruses cause loss of data, destroy computer hardware, create negative impacts to computer networks and systems, and disrupt business, government, and personal affairs. In the battle against computer viruses, an entire industry was created to develop and sell “anti-virus” software to detect, remove, and insulate computers from viruses. Numerous patents have been granted to achieve these same goals. Examples of corporations within the anti-virus industry are Symantec and Network Associates. Currently, the control of viruses is dependent upon companies such as these to identify characteristics of viruses, write anti-virus software to detect viruses when encountered, and insulate computers from viruses. However, viruses are created faster than anti-virus software, and anti-virus software cannot always prevent outbreaks of virus infections. It is desirable to avoid the negative impacts of virus infections without reliance on software that needs to continually adapt to detect new specific viruses.

What Are Computer Viruses?

A computer virus is a program that invades computer host systems. Once inside a host system, the virus may replicate and create copies of itself. The virus may also cause damage to the host system. Viral programs can damage host systems by using the host file system to over-write data in host systems, or over-write data stored in networks attached to host systems, or create numerous other disruptions or damage. In addition to damaging the host system, the virus may perpetuate itself by transmitting replicated copies to other computer systems. Most computer viruses use e-mail systems to transmit the replicated copies to other computer systems. By transmitting replicated copies of itself to other computer systems, the virus invades new host systems and continues the life-cycle of viral replication, host system damage, and transmission of duplicate virus programs.

How Computer Users Spread Viruses:

E-mail systems alone cannot activate viral programs within host systems. Viral programs require activation by computer users, and therefore viral programs are sent as file attachments to e-mail messages. The creators of the viral programs rely on computer users to open the infected file attachments. The viral programs activate when users open infected attached files. The term “open” means the user starts the program in the attachment or starts a program associated with the attachment. In Microsoft Windows and NT operating systems, data files are named in a two part format of the form xxxxxxxx.yyy, where the “.” separates the user given name, “xxxxxxx”, from the extension, “yyy”. The operating system uses the extension, “yyy”, to select how the data file is to be treated when opened. For example if the extension is “exe”, then the operating system treats the data file as an executable program and passes control to it when opened. Or, if the extension is “doc”, the operating system associates the document with the Microsoft Word program, loads the Microsoft Word program, and passes control to the Microsoft Word program with the data file as an input file.

What Are Viral Infected E-Mail Attachments?

Viral infected e-mail attachments are of two types: 1) programs that execute when opened or 2) “macros” that execute when data files are opened as documents in other programs such as Microsoft Word. A macro is a program that is written in a language specific to another program such as Microsoft Word. Macros are used to automate sets of “user actions”. Examples of macro “user actions” are the ability to open and write data files, and to send e-mail messages with attachments to recipients in the users’ e-mail directories. Viral macros may use the previously described user actions and other functions to send replicated copies of itself as attachments to other e-mail users. The infected attachments may cause damage to data in the host system or to data in a network that is attached to the host system.

Life-Cycle of Computer Viruses:

The key to life or the goal of viruses is to replicate and transmit copies of itself to other computer systems. There are viral programs that can access the computer users’ e-mail directory and the computer users’ e-mail folders. This access allows the virus to send additional replicated viral attachments to associates of the user. The viral e-mail messages appear to originate from

someone the recipient knows and trusts, when in fact the virus sends the e-mail message itself. The unsuspecting recipient opens the infected files due to the mistaken belief that the file is virus-free merely because the e-mail was sent from a familiar e-mail address. The opened and activated virus file repeats its cycle, and the virus succeeds in its continuous spread to other computer systems.

What Is Being Done?

Anti-virus companies such as Symantec and Network Associates attempt to stop viruses with the detection, removal, and insulation of computer viruses. Additionally, software creators of e-mail systems attempt to curb the spread of viruses by building features into e-mail programs that attempt to prevent the opening of viral attachments. For example, Microsoft Corporation added capabilities to recent releases of Outlook and Exchange e-mail programs that makes opening attachments with executable programs a two-step process. In the Microsoft Outlook e-mail program, an attachment to an e-mail appears as an icon in the body of the e-mail. The file name appears as text in the icon. The user "opens" the attachment by double clicking on the icon. The first step consists of a warning message that is displayed when the icon is double-clicked. The user must perform a second action to actually open the file. Consistent with this, recent releases of Microsoft Word and Excel have a similar two-step document opening process if there is a macro in the document. First the user is warned that there is a macro in the document. The second step requires the user to choose to not open the document, disable the macro and open the document, or open the document with an active macro. In spite of these virus avoidance measures, computer users continue to open attachments with viruses, which in turn harms their systems, and sends replicated viral copies to other unsuspecting computer systems. An article written by David L. Wilson and published in the December 4, 1999 edition of the *San Jose Mercury News* is included as background information on how computer viruses damage, replicate and spread.

BRIEF SUMMARY OF THE INVENTION

The dangerous computer virus phenomenon cannot be neutralized solely by the use of software programs that detect and remove computer viruses, or by functions within e-mail programs that warn against opening potentially harmful files and attachments. Nearly all computer viruses require action by computer users in order for the viruses to infect and spread. Therefore computer users must change their behavior to stop viruses. Our invention is a tool that teaches computer users to avoid computer viruses with the use of mock computer viruses. The invention can aid, test, and reinforce behavior changes. The invention can also measure the effectiveness of behavior change in an organization or e-mail population by collecting and analyzing feedback measurements.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING

An article written by David L. Wilson and published in the December 4, 1999 edition of the *San Jose Mercury News* is included as background information on how computer viruses damage, replicate and spread. The article demonstrates that attempts are made by the mass media to educate computer users to avoid computer viruses. Despite the widespread information available to users on how to avoid computer viruses, the advice is left unheeded and the viruses continue to damage, replicate, and spread. The article is labeled as Drawing 1.

DETAILED DESCRIPTION OF THE INVENTION

Computer Users Spread Computer Viruses:

Nearly all computer viruses require action by computer users for the viruses to infect and spread. The key to controlling viruses is to educate users not to open file attachments that might carry viruses. Education about how to avoid computer viruses is similar to education about how to avoid incurable human viral diseases. For example, in some cases of human disease, there are human behaviors that can eliminate or minimize exposure to infectious disease. Computer viruses are similar in that behavior modification on the part of computer users can greatly eliminate or minimize exposure to computer viruses. However, education alone is an ineffective tool to stopping viruses. There are many widely published writings and documents, such as the

San Jose Mercury News article, that warn of the danger of opening computer viral attachments yet many people continue to open infectious attachments. Effective behavior modification must have a means to reinforce the change, and to measure how widespread the change is in a population.

Changing Human Behavior is the Key to Conquering Computer Viruses:

In general, most computer users do not need to send executable programs as attachments or documents with macros to other e-mail users. One behavior change is that a user should not send executable programs or documents with macros unless absolutely necessary. If it is necessary to send such attachments, the sender needs to communicate to the recipient to expect specific attachments. The second, and most important, behavior change is that a user should not open an attachment that is an executable program or a document with a macro unless there is specific knowledge that the attachment is safe to open. The third behavior change is that a user should inform their information services staff if they receive an e-mail attachment that appears to contain a computer virus. This last behavior provides early warning of new computer viruses, and allows companies such as Symantec and Network Associates to update their anti-virus software detection programs before the virus becomes widespread.

How Behavior Changes can be Made, Measured and Tracked:

Our invention tests, reinforces, and measures the changes in computer user behavior in regards to viral attachments, or attachments that may carry viruses. The invention sends e-mail messages with attachments to e-mail users. The attachments look similar to attachments that carry computer viruses. The invention creates a list of all users that open the attachment. If the attachment is opened, an e-mail is sent to a specific e-mail address – perhaps that of an Information Systems manager who will monitor behavioral changes. This specific e-mail address collects all of the e-mail addresses and information from users who have not changed their behavior and need additional education or management attention. Additionally, a message within the attachment is displayed to the e-mail user informing them they opened a file that may have contained an infected virus. The e-mail user may also receive a separate e-mail message informing them again that they opened a file that may have contained an infected virus.

It is possible to test, measure, and track behavioral changes of an entire e-mail user population of a corporation for example, or randomly sample a small portion of an e-mail community. E-mail systems such as Microsoft Outlook have the ability to track when a user receives an e-mail message, opens an e-mail message, and/or deletes an e-mail message. However these e-mail tracking functions only apply to the e-mail messages and not to the attachments. The behaviors of e-mail users, such as deletion of the invention e-mail, can be tracked and measured. In addition, for behavior reinforcement, the attachment can display a message that warns the user that they have opened an attachment that could have been a computer virus. The attachment can also act very similar to a computer virus and replicate itself and transmit copies to other e-mail addresses (secondary e-mail addresses). Secondary e-mail addresses can be gathered from the original user's personal e-mail directories. It will appear to the secondary e-mail recipients that the email attachments originated from people that the secondary recipients might know, when in fact the e-mail messages and attachments originated from the invented viruses. These actions are similar to the behavior of real computer viruses and they will test an organization for safe computer behavior. To limit the impact of the computer virus replication process, the invented virus may contain a counter that changes with each replication cycle. The replication process can cease after a specified number of cycles.

The Concept and Design of the Invented Virus:

The invention is basically a benign computer virus, and therefore must be designed to pass undetected by anti-virus software and be attractive for e-mail users to open. Since anti-virus software is continuously updated and user behavior will become more sophisticated, the invention must also be continuously updated to mimic harmful "wild" computer viruses.

The basic elements of the invented benign virus can be implemented as executable programs written in C++, Visual Basic, or a number of programming languages that contain programming functions that use Mail Application Programming Interface, MAPI. The invention uses MAPI to send feedback e-mail information to a specific e-mail address of a person who will monitor, measure, and track computer user behavior (i.e. the person who will perform the "tracking function" –for example an Information Systems administrator). The invented program

is sent as an attachment to the e-mail users. The invention can also be implemented as a Microsoft Word macro in a Word document using macros such as “File”, “Send to”, or “Mail Recipient” functions. The macros can send e-mail feedback to the person performing the “tracking function”.

The design of the benign virus can be crafted from virulent viruses to mimic their appearance and replication capabilities. The virulent virus would be modified to send the e-mail information to the person performing the tracking function, and the destructive functions would be deleted. The virulent virus may also need to be modified to circumvent anti-virus programs. The resulting benign virus is sent as an e-mail attachment to the test population. The person performing the tracking function will receive e-mails in his/her e-mail “in-box” from all of the users who open the attachment. The tracking function person’s e-mail “in-box” can be used to generate a list of users who need additional attention and behavior modification. The steps of creating the e-mail user list to be tested, sending the e-mails, and creating the list of e-mail users may be done as manual steps or automated as a program using the MAPI functions.

One key element in the battle against computer viruses is changing user behavior to prevent opening infected e-mail attachments. This invention aids in reinforcing and measuring changes in user behavior.

CLAIMS:

We claim ...

1. A computer virus avoidance system that sends an e-mail with an attachment to e-mail users and creates a list of e-mail users that open the attachment.
2. The computer virus avoidance system of claim 1, wherein the attachment displays a message to the user when the attachment is opened.
3. The computer virus avoidance system of claim 1, wherein an e-mail message is sent to users that open the attachment.
4. The computer virus avoidance system of claim 1, wherein the attachment transmits replications of itself to other e-mail users.
5. The computer virus avoidance system of claim 4, wherein the number of replication and transmission cycles is limited.
6. A computer virus avoidance system and an e-mail system, comprising: a means for sending an e-mail with an attachment to an e-mail address, and a means to send an e-mail to a specific e-mail address when the attachment is opened.
7. The computer virus avoidance system of claim 6, wherein the attachment displays a message to the user when the attachment is opened.
8. The computer virus avoidance system of claim 6, wherein an e-mail message is sent to users that open the attachment.
9. The computer virus avoidance system of claim 6, wherein the specific e-mail address gathers and creates a list of e-mail users that opened the attachment.
10. The computer virus avoidance system of claim 6, wherein the attachment contains a means to send a replica of itself to another e-mail address.
11. The computer virus avoidance system of claim 10, wherein the number of times that the attachment replication process is limited.

12. A computer virus avoidance system in a computer network and a system for sending an e-mail wherein an e-mail is sent to an e-mail address, and the e-mail has an attachment that sends an e-mail to a specific address when the attachment is opened.
13. The computer virus avoidance system of claim 12, wherein the attachment displays a warning message to the user when the attachment is opened.
14. The computer virus avoidance system of claim 12, wherein an e-mail message is sent to users that open the attachment.
15. The computer virus avoidance system of claim 12, wherein the specific e-mail address is that of an e-mail "in-box" that creates a list of e-mail addresses that have sent it messages.
16. The computer virus avoidance system of claim 12, wherein the attachment sends a replica of itself to another e-mail addresses.
17. The computer virus avoidance system of claim 16, wherein the number of replication cycles is limited.

ABSTRACT OF THE DISCLOSURE

Nearly all computer viruses require an action by a computer user to infect and spread. The key is to educate users not to open e-mail attachments that might carry computer viruses. The key is behavior modification, as education is not sufficient. Effective behavior modification must have a means to reinforce the change and to measure how widespread the change is in a population. The invention is used to reinforce and measure the change in user behavior. The invention sends an e-mail with an attachment to e-mail users and creates a list of all users that open the attachment. The user is sent an e-mail with an attachment that looks similar to attachments that contain computer viruses. If the attachment is opened, an e-mail is sent to a specific e-mail address. This e-mail address collects all of the e-mail from users who have not changed behavior and need additional education or management attention.

662221-33002460

Holiday e-mails can carry a danger

Experts are warning about viruses in infected attachments

BY DAVID L. WILSON

Mercury News Washington Bureau

WASHINGTON — The holiday season is often a time when computer users pass around amusing electronic animations via e-mail. Although most of these attachments are harmless, some may hide destructive computer viruses.

Indeed, anti-virus watchdogs identified a new virus this week that masquerades as an innocuous bunch of digital photos but actually plants a time bomb that will erase the computer's hard drive on Jan. 1, 2000.

Because that's the same date that the Y2K bug is expected to cause many computer systems to crash, the virus might fool users into believing they have a Y2K problem.

Virus fighters expect more viruses linked to Y2K to emerge as Jan. 1 approaches, and they are once again begging computer users to avoid opening e-mailed attachments.

"We're telling people to be very wary of electronic Christmas cards," said Sal Viveros, a virus expert with Network Associates Inc., based in Santa Clara.

The Mypics worm, as this latest threat is called, arrives attached to what appears to be e-mail from a friend or associate that says, "Here's some pictures for you!"

Opening the attached file, Pics4You.exe, will infect your computer with the virus, which will at-

See **VIRUSES**, Page 3C

Y2K PROBLEM



Virus fighters

expect more

viruses

linked to Y2K

to emerge as

Jan. 1

approaches.

Holiday e-mails carry risk

■ VIRUSES

from Page 1C

tempt to mail itself to 50 people it finds in your Microsoft Outlook e-mail address book. It will also change the home page of your Microsoft Internet Explorer Web browser to a pornographic site.

The real damage occurs Jan. 1, when the virus will change the computer's most basic software and attempt to erase the hard drive.

The increasing frequency of alerts relating to things like electronic viruses is prompting renewed calls for safe computing, but few experts expect users to change their habits.

"It would be great if everybody followed the rule: Never open e-mail attachments if you can help it," said Carey Nachenberg, chief researcher at Symantec's anti-viral research center. "But I don't think they will."

In general, just looking at an infected e-mail can't hurt; users have to do something else to activate the virus and infect their system. Typically, a virus comes as an attachment to e-mail, such as a document that can be read only with a word processor like Microsoft Word.

Clicking on the attachment to read the document can infect the user's machine with any virus that was lurking on the sender's machine. A virus is dangerous because it can alter or destroy data.

Until recently, experts advised users to simply avoid opening attachments sent by people they didn't know. Unfortunately, the most troublesome viruses today spread by fooling people into believing the document was sent by a friend.

For instance, Mypics attempts to mail copies of itself to anyone in the user's e-mail address book. Anyone receiving such a missive from, say, their brother, might open that attachment without thinking about it.

Most software vendors are aware of the problem and take steps to get around it. For instance, Blue Mountain Arts, a purveyor of electronic greeting cards, doesn't send the card via e-mail, just a Web address, which can be accessed through any browser.

Jared P. Schutz, the company's executive director, said that's the only way to be safe. "I would highly recommend that people avoid opening attached files, even from people that they know," he said.

A computer virus for Christmas

Many computer viruses travel as innocent looking files attached to electronic mail. With the holiday season upon us, people often e-mail electronic greetings and photographs to friends and family members, but not every file that comes with an e-mail is safe. This year poses special hazards, according to anti-virus experts, because many virus writers may use the Y2K bug to hide their mischief. This week, anti-virus companies detected a new virus, named Mypics, that could erase a computer's hard drive on Jan. 1.



Infected e-mail attachment



1 WORM ARRIVES

You get an e-mail with an attachment named Pics4You.exe saying, "Here's some pictures for you!"



Infected computer



2 WORM REPRODUCES

If you open the attachment, the worm will send itself to 50 people in your Microsoft Outlook address book. It also changes the home page of your Microsoft Internet Explorer browser to a pornographic site.



3 WORM WAITS

On Jan. 1, 2000, the worm will overwrite key system data. The user will see an apparent Y2K-related error when starting up the computer. The worm will then destroy all data on the hard drive.

HOW TO PROTECT YOURSELF

Avoid opening attachments to e-mail if possible. If you want the attachment, call the sender and verify its contents before opening it. Update virus protection software weekly and use it to scan attachments. Back up critical data regularly.

Source: Symantec Corp.

MERCURY NEWS

That's the standard advice, but nobody expects attachments to disappear tomorrow, despite the warnings.

"I can't tell you whether we've still got a lot of people who just haven't gotten the message — newbies — or whether it's people who should know better but do it anyway," said Sandra Sparks, director of the Energy Department's Computer Incident Advisory Capability, which works to ensure the security of government computer systems. "Maybe it's the same kind of thing that happens with people who don't wear a seat belt."

Although many corporations scan all incoming e-mail and destroy any known virus before it's delivered into an employee's mailbox, very few Internet service providers offer such a feature, largely because examining every single data packet that flows into the pipes can slow service.

So for now, anti-virus protection is largely the responsibility of individuals.

To protect against all viruses, experts say virus protection software should be updated weekly.

Attachments generally should be avoided. If you receive an attachment that you want, contact the sender and ask if it was deliberately sent. If possible, ask that the information in the attachment be copied and pasted into a plain e-mail file and resent or posted on a Web page.

If that's not possible and you must open the attachment, make sure it's scanned first with an updated anti-viral program.

Even with such precautions, it's still possible for a new, fast-moving virus to get through your defenses. The only real protection users have is to regularly make copies of the data on their hard drive.

"Back up your critical stuff at least once a week," said Sparks. "I know that's annoying, and I know it takes time. But compare that amount of time vs. the amount of time you'd spend trying to rebuild your system, or your company, and that's a very small investment."

Contact David Wilson at (202) 383-6020 or at dawilson@sjmercury.com.

Please type a plus sign (+) inside this box → ☐

PTO/SB/01 (12-97)

Approved for use through 9/30/00. OMB 0651-0032

Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number

**DECLARATION FOR UTILITY OR
DESIGN
PATENT APPLICATION
(37 CFR 1.63)**

☒ Declaration Submitted with Initial Filing **OR** ☐ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number

First Named Inventor

KIMBERLY J. WELBORN

COMPLETE IF KNOWN

Application Number

/

Filing Date

Group Art Unit

Examiner Name

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

COMPUTER VIRUS AVOIDANCE SYSTEM AND MECHANISM

the specification of which

(Title of the Invention)

☒ is attached hereto
OR

☐ was filed on (MM/DD/YYYY) as United States Application Number or PCT International

Application Number- and was amended on (MM/DD/YYYY) (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below

Application Number(s)	Filing Date (MM/DD/YYYY)	<input type="checkbox"/> Additional provisional application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

[Page 1 of 2]

Burden Hour Statement This form is estimated to take 0.4 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box → ☐

PTO/SB/01 (12-97)
Approved for use through 9/30/00. OMB 0651-0032
Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

I hereby claim the benefit under 35 U.S.C. 120 of any United States application(s), or 365(c) of any PCT international application designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

U.S. Parent Application or PCT Parent Number	Parent Filing Date (MM/DD/YYYY)	Parent Patent Number (if applicable)

☐ Additional U.S. or PCT international application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

As a named inventor, I hereby appoint the following registered practitioner(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

☐ Customer Number

OR

☐ Registered practitioner(s) name/registration number listed below

Place Customer
Number Bar Code
Label here

Name	Registration Number	Name	Registration Number

☐ Additional registered practitioner(s) named on supplemental Registered Practitioner Information sheet PTO/SB/02C attached hereto.

Direct all correspondence to: ☐ Customer Number or Bar Code Label ☒ Correspondence address below

Name	KIMBERLY JOYCE WELBORN				
Address	331 SANDPIPER DRIVE				
Address					
City	DAVIS	State	CA	ZIP	95616
Country	U.S.A.	Telephone	530.753.7240	Fax	530.757.9200

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name of Sole or First Inventor: ☐ A petition has been filed for this unsigned inventor

Given Name (first and middle (if any))		Family Name or Surname					
KIMBERLY JOYCE		WELBORN					
Inventor's Signature	<i>Kimberly Joyce Welborn</i>		Date	12/22/99			
Residence: City	DAVIS	State	CA	Country	U.S.A.	Citizenship	U.S.A.
Post Office Address	331 SANDPIPER DRIVE						
Post Office Address							
City	DAVIS	State	CA	ZIP	95616	Country	U.S.A.

☒ Additional inventors are being named on the 1 supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto

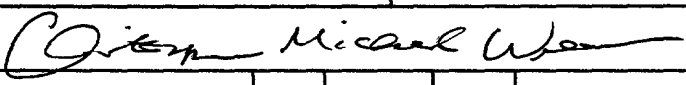
Please type a plus sign (+) inside this box → ☐

PTO/SB/02A (3-97)
Approved for use through 9/30/98. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number

+

DECLARATION

ADDITIONAL INVENTOR(S)
Supplemental Sheet
Page 1 of 1

Name of Additional Joint Inventor, if any:		<input type="checkbox"/> A petition has been filed for this unsigned inventor					
Given Name (first and middle [if any])				Family Name or Surname			
CHRISTOPHER MICHAEL				WELBORN			
Inventor's Signature						Date	12/22/1999
Residence: City	DAVIS	State	CA	Country	U.S.A.	Citizenship	U.S.A.
Post Office Address	331 SANDPIPER DRIVE						
Post Office Address							
City	DAVIS	State	CA	ZIP	95616	Country	U.S.A.
Name of Additional Joint Inventor, if any:		<input type="checkbox"/> A petition has been filed for this unsigned inventor					
Given Name (first and middle [if any])				Family Name or Surname			
Not Applicable							
Inventor's Signature						Date	
Residence: City		State		Country		Citizenship	
Post Office Address							
Post Office Address							
City		State		ZIP		Country	
Name of Additional Joint Inventor, if any:		<input type="checkbox"/> A petition has been filed for this unsigned inventor					
Given Name (first and middle [if any])				Family Name or Surname			
Not Applicable							
Inventor's Signature						Date	
Residence: City		State		Country		Citizenship	
Post Office Address							
Post Office Address							
City		State		ZIP		Country	

Burden Hour Statement: This form is estimated to take 0.4 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231

66222T-3502460

+